1/23

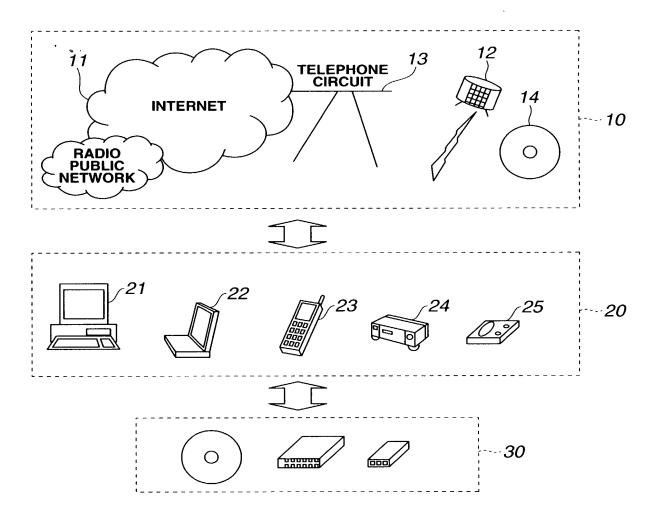


FIG.1

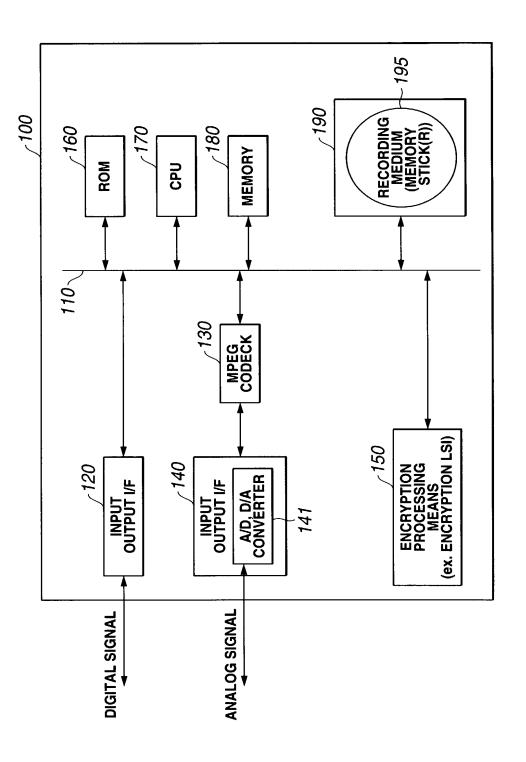
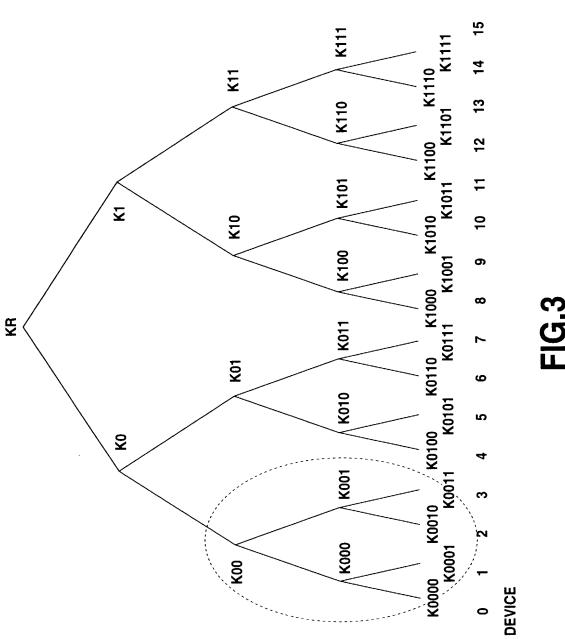


FIG.2



4/23

| VERSION : t | | |
|-------------|----------------------|--|
| INDEX | ENCRYPTED KEY | |
| 0 | Enc(K(t)0, K(t)R) | |
| 00 | Enc(K(t)00, K(t)0) | |
| 000 | Enc(K000, K(t)00) | |
| 001 | Enc(K(t)001, K(t)00) | |
| 0010 | Enc(K0010, K(t)001) | |

FIG.4A

| VERSION: t | |
|------------|----------------------|
| INDEX | ENCRYPTED KEY |
| 000 | Enc(K000, K(t)00) |
| 001 | Enc(K(t)001, K(t)00) |
| 0010 | Enc(K0010, K(t)001) |

FIG.4B



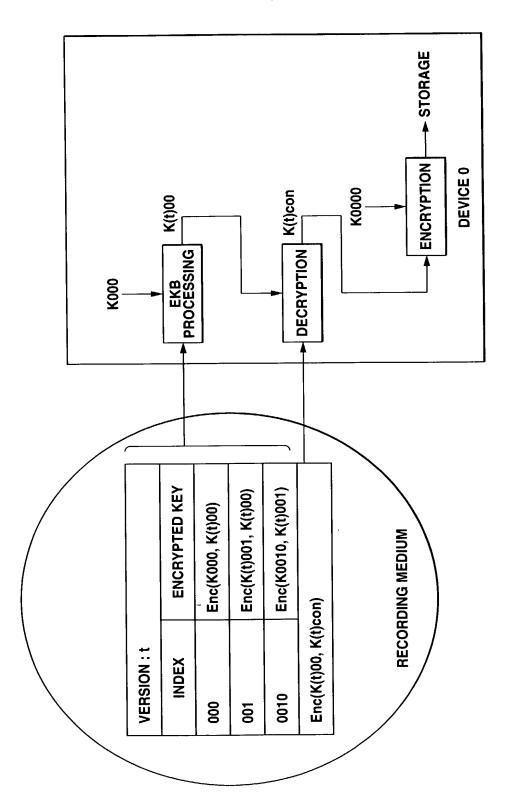


FIG.5

6/23

| | | | • |
|--------------|-----------------------------|-------------|---------------|
| 601~ | VERSION | DEPTH | ~602 |
| 603~ | DATA POINTER | TAG POINTER | ~- <i>604</i> |
| <i>605</i> ~ | SIGNATURE POINTER | RESERVED | |
| , | DATA PART (E(K0, Kroot),) | | |
| | TAG PART ({0, 0}, {1, 1},) | | |
| | SIGNATURE | | |

FIG.6

7/23

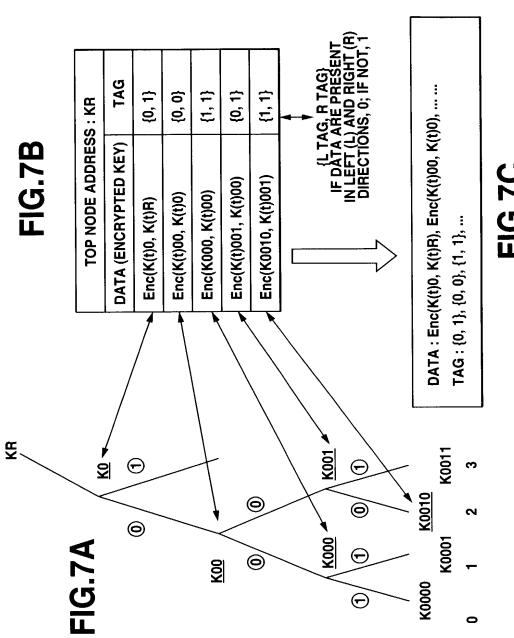
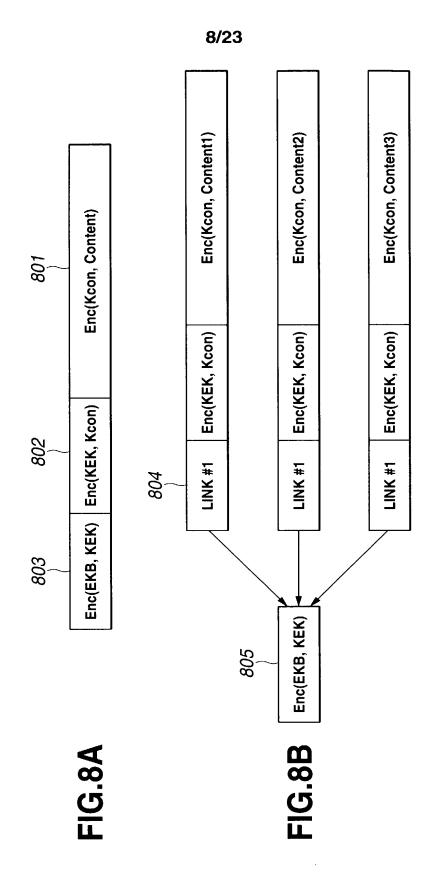


FIG.7C



9/23

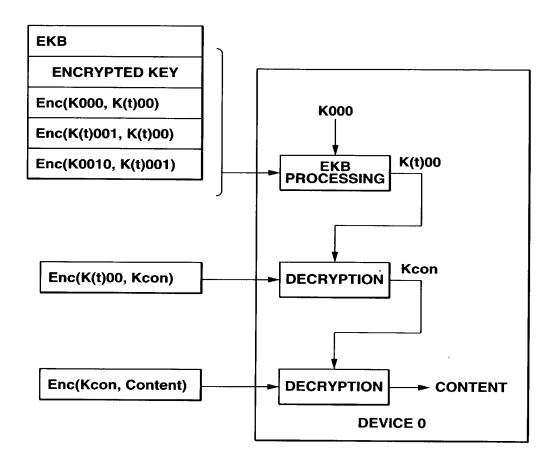


FIG.9

10/23

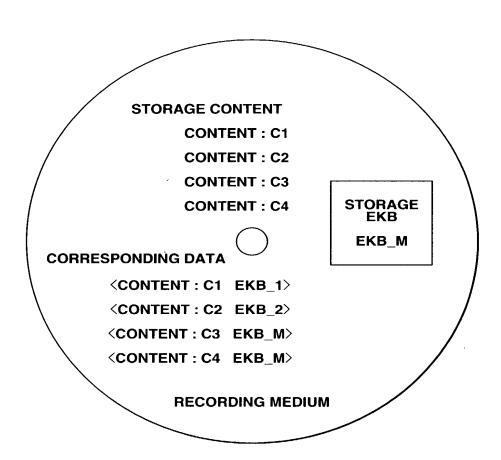
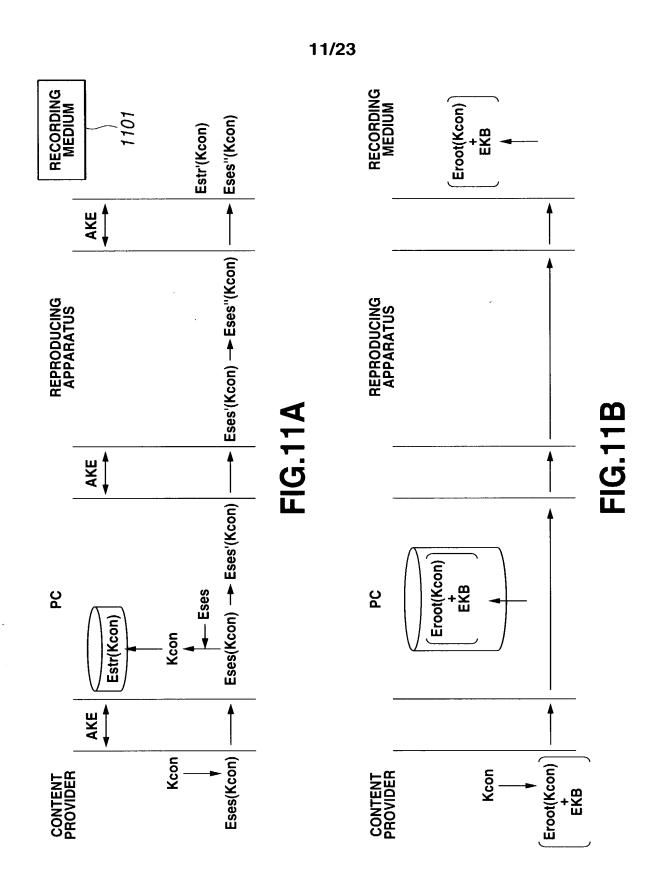


FIG.10



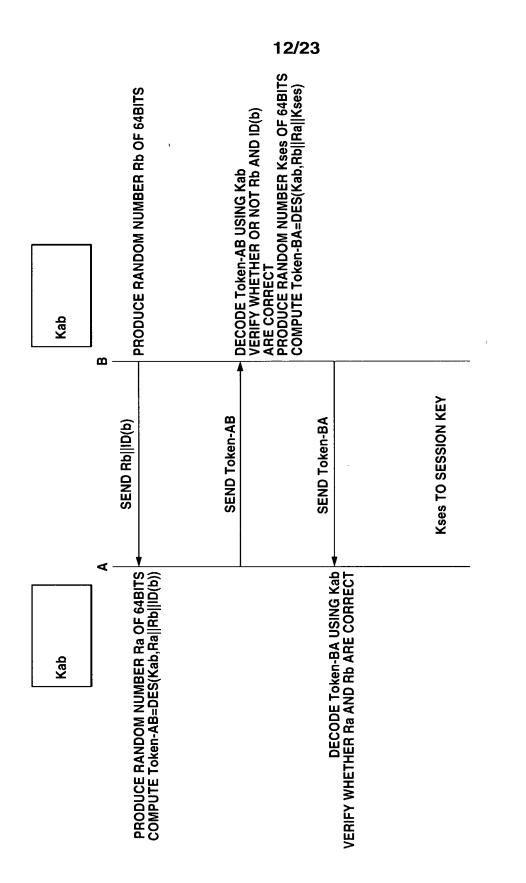


FIG.12

13/23

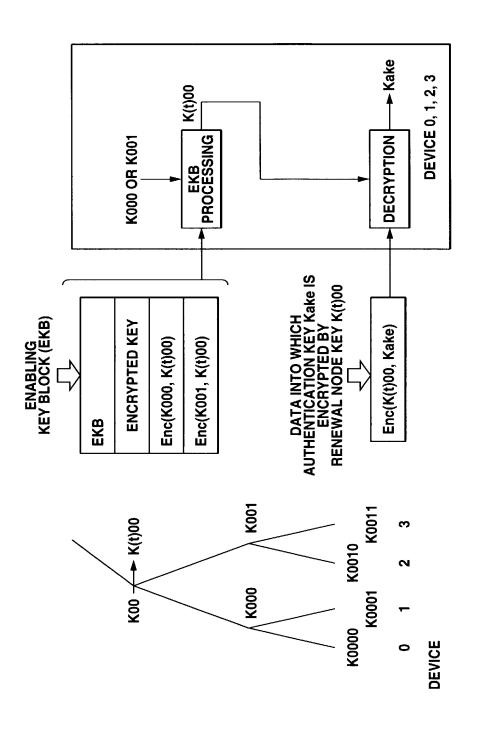


FIG. 13

14/23

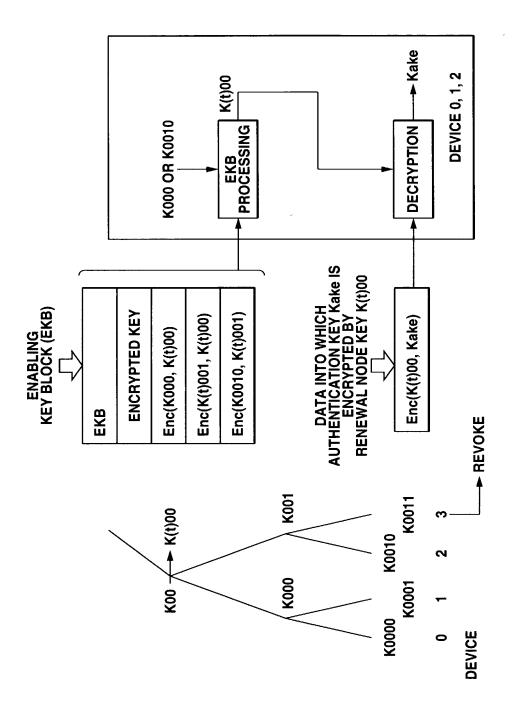


FIG.14

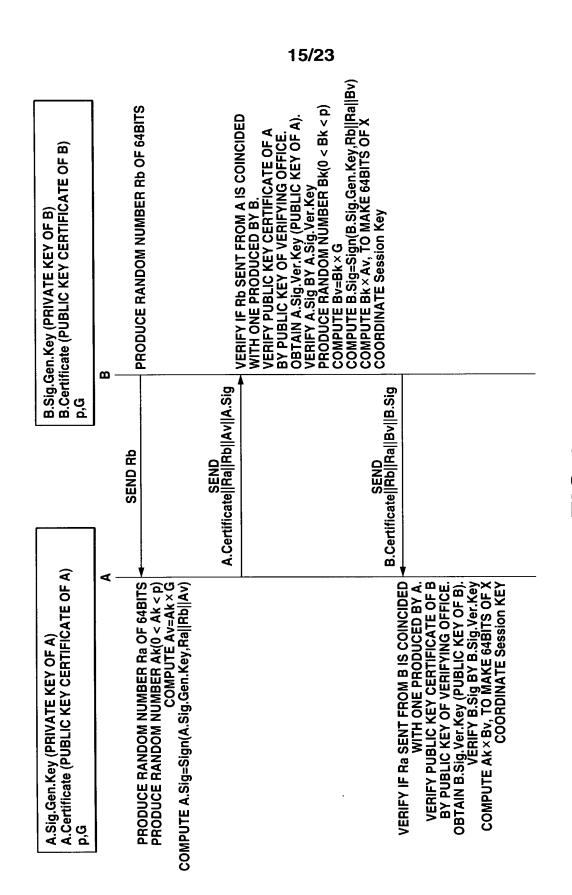


FIG.15

16/23

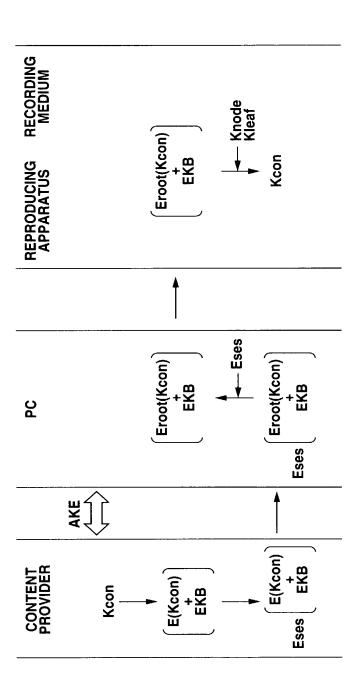


FIG.16

17/23

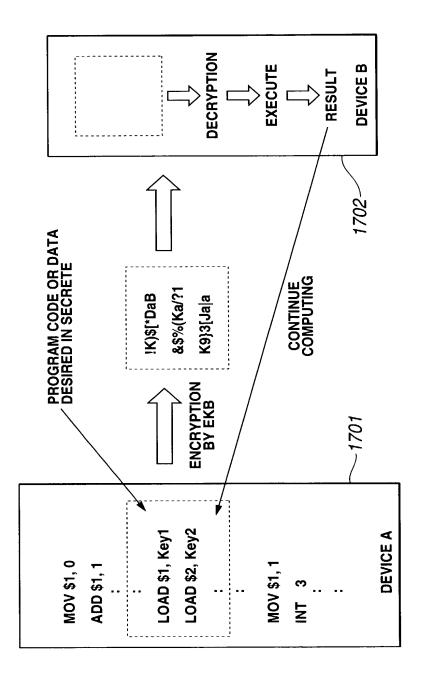
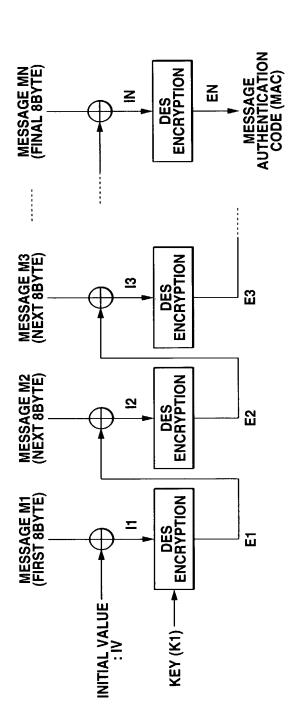


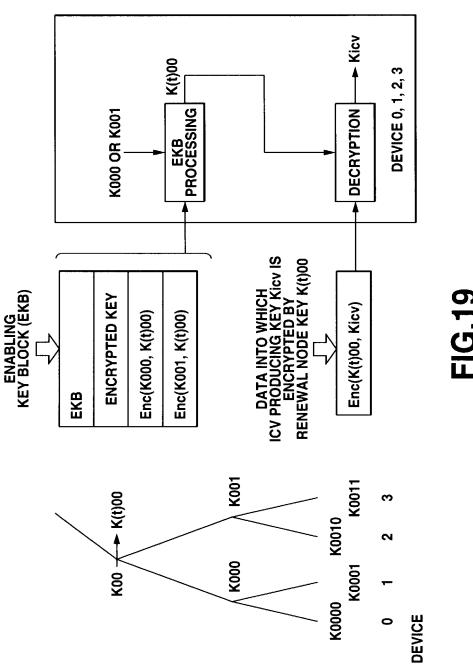
FIG.17

18/23

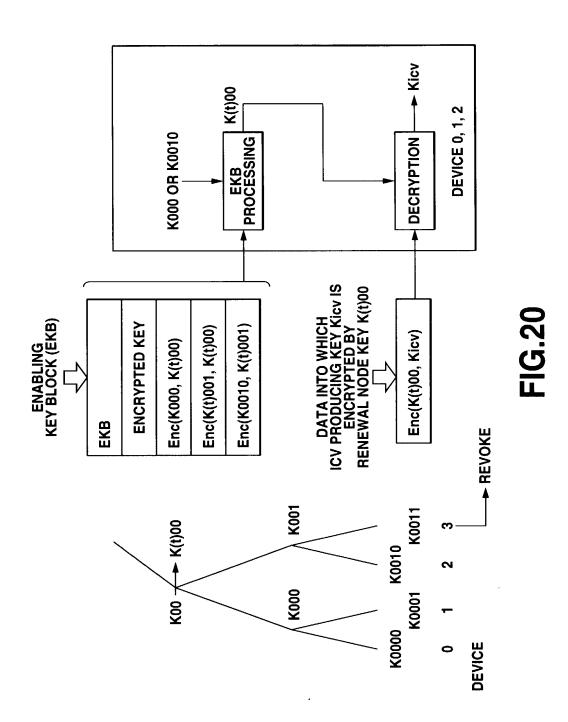


⊕ : EXCLUSIVE OR PROCESSING (8BYTE UNIT)

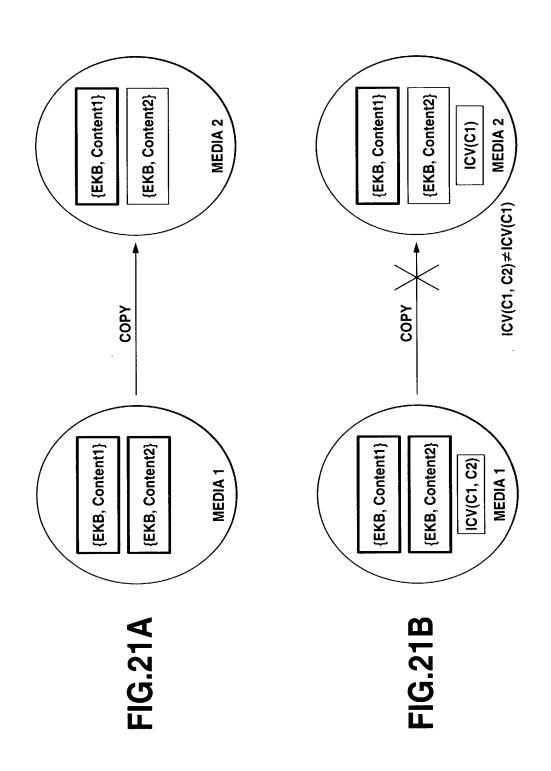
19/23



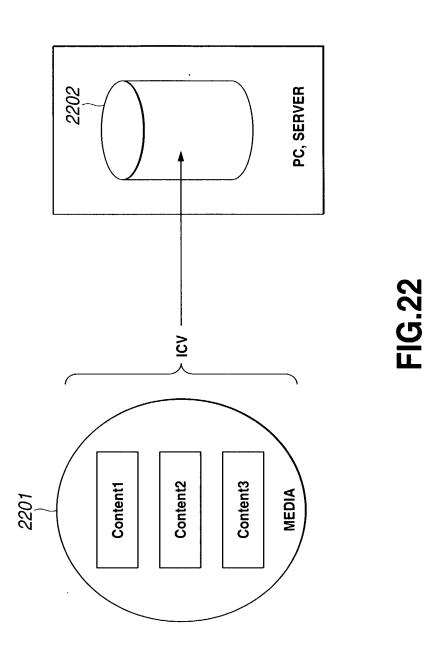
20/23



21/23



22/23



23/23

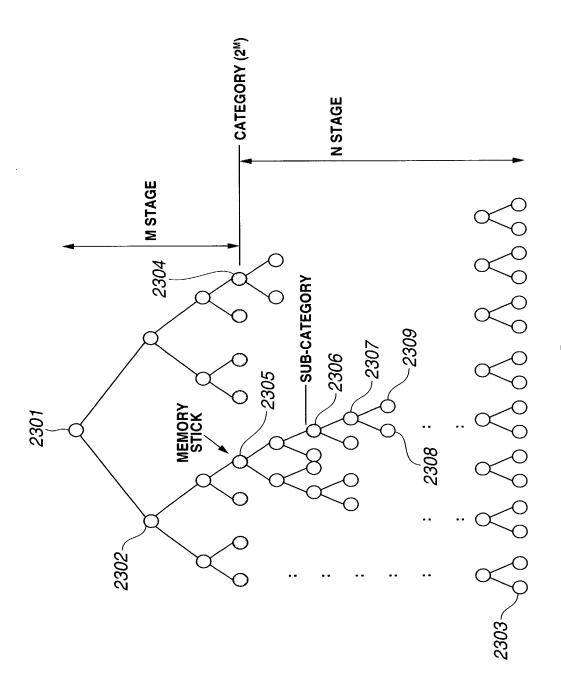


FIG.23